

Joint encryption/watermarking based on Arnold cat map and DCT

Hema S Meharwade, Veena S, Arathi R Shankar

M.Tech 4th sem Student, Principal Scientist, Associate Professor

BMSCE Bengaluru, CSIR- National Aerospace Laboratories Bengaluru, BMSCE Bengaluru

hemameharwade@gmail.com, veenas @ nal.res.in, arathi.ece@bmsce.ac.in

Abstract—This paper presents a joint encryption and watermarking technique for images. The encryption algorithm is based on Arnold transformation and S-box substitution and the watermarking technique is carried out in the DCT domain. The results show the performance of algorithm in terms of correlation function and differential attack.

Keywords - Data protection, Encryption, Decryption, DCT watermarking, Arnold Cat transformation, S-Box

I. INTRODUCTION

In today's world it is very much essential to secure the data being transmitted over a communication channel and this can be accomplished by two schemes: Encryption and watermarking. Encryption gives techniques for securing the integrity and authenticity of transfer of information. Encrypted data cannot be interpreted and need to be decrypted at the receiving end. Therefore, in addition to encryption, a Watermarking technique is used for embedding hidden copyright protection information to digital information being transmitted. These two techniques are complementary rather than overlapping and can be combined to increase protection of the message [1].

Encryption/cryptographic algorithms use two main techniques known as **substitution** and **permutation** [2]. Substitution is simply a mapping of one value to another and permutation is a reordering of the bit positions for each of the inputs. These techniques are used a number of times in iterations called **rounds**. Generally, the more rounds there are, the more secure the algorithm. A non-linearity is also introduced into the encryption so that decryption will be computationally infeasible without the secret key. This is achieved with the use of **S-boxes** which are basically non-linear substitution tables where either the output is smaller than the input or vice versa. The standard methods such as AES and DES are highly secure data encryption algorithms [3]. However they are computationally intensive for image and video encryption. Several image encryption algorithms are available in the literature. Among them chaotic maps and cryptographic algorithms have some similar properties

like Pseudo-random behavior, sensitivity to initial conditions and parameters and unstable orbits with long periods, depending upon the precision of the numerical implementation [4]. Encryption rounds of a cryptographic algorithm lead to diffusion and confusion properties. In a similar manner, iterations of the chaotic map spread the initial region over the entire phase space. In this respect, chaos based encryption techniques are considered good for practical use. Existing Chaotic methods are based on schemes like 2D standard Barker map, BRIE, Chaotic Key generation, cat maps, Arnold transforms etc[5].

Digital image watermarking algorithm includes four categories: time-domain (e.g. LSB, Patchwork algorithm), compressed domain (e.g. JPEG, MPEG, transform domain (e.g. DCT domain, DWT domain) and spread spectrum watermarking. The DCT domain watermark algorithm has good hidden effect, can not only withstand loss JPEG compression, filtering, signal processing, but also subject to the general geometric transformation, such as cropping, scaling, translation and rotation operations. Its robustness is good and computational complexity is low[6].

A joint encryption watermarking scheme combines both the techniques to ensure security and copyright protection, from the point of view of achieving double security and reduced computational complexity.

In this paper, a joint encryption watermarking scheme based on Arnold S-box method of [7] and DCT domain watermarking is proposed.

II. ARNOLD CAT MAP AND S-BOX

The method adapted is referred from [7]. Here, Arnold cat map is used to shuffle the pixel positions and to disturb the high correlation among the image pixels. Further, the concept of S-box of AES is used in substitution phase to increase the nonlinearity and these result in a robust algorithm.

The Arnold transformation is given as

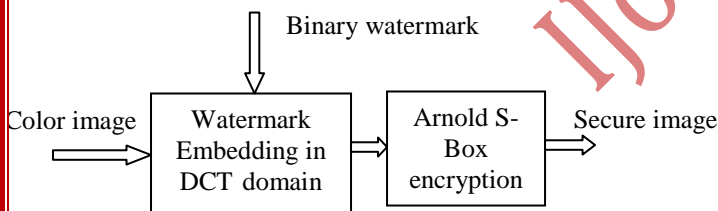
$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & pq + 1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \text{ mod } N \dots\dots\dots [1]$$

Where p and q are positive integers and (x', y') is the new positions of the original pixel position (x, y) when Arnold cat map is performed once. The result after applying the Arnold Cat Map for number of iterations iterating R will be a shuffled image that contains all of the same pixel values of the original image. The number of iteration R to be satisfied that depends on the parameters p, q and the size N of the original image. Thus the Arnold cat map's parameters p, q, and the number of iterations R, can be used as the secret keys. After this stage an S-box [7] is used for substitution.

III. DCT WATERMARKING

The DCT allows an image to be broken up into different frequency bands, making it much easier to embed watermarking information into the middle frequency bands of an image[8]. The middle frequency bands are chosen such that they avoid the most visual important parts of the image (low frequencies) without over-exposing themselves to removal through compression and noise attacks (high frequencies)[9].

IV. PROPOSED JOINT ENCRYPTION/WATERMARKING METHOD



The proposed scheme is a combination of Arnold cat map and S-box substitution and DCT watermarking. Figure 1. illustrates the block diagram of the proposed algorithm.

An algorithm steps which is shown in figure are given below:

1. Watermarking stage

- Step1: the original Image is resized it into a 512X512 matrix
- Step2: watermark image is resized it into a 64X64 matrix.

Step3: The resized original image is segmented into 8X8 sub-blocks and DCT of each sub-block is computed

Step5: The watermark is embedded into original image using the formula

$$F(m, n) = \alpha * w(x, y) \quad \alpha - \text{strength factor}$$

Step5: The IDCT function is used to achieve watermarked image

2. Encryption stage

Step-1: Generate S-box and define k(number of iterations carried out) value

Step -2: Read the watermarked image.

Step -3: Apply Arnold transformation followed by S-box to achieve encryption

The decryption algorithm is same as encryption but with replacing the Arnold transformation with its inverse and using the inverse S-box table. The watermark can be extracted using the formula

$$w(x, y) = F(m, n) / \alpha$$

A. Performance Evaluation of encryption algorithm

1) Encryption Quality

The encryption quality represents the average number of changes to each grey level L

$$\text{Encryption Quality} = \frac{\sum_{L=0}^{255} |HL(E) - HL(P)|}{256} \dots [2]$$

P, E - original, encrypted images of size M*N pixels with L grey levels.

HL(P), HL(E) - number of occurrences of each grey level L in P and E

2) Analysis of correlation of two adjacent pixels

A correlation is a statistical measure of security that expresses a degree of relationship between two adjacent pixels in an image or a degree of association between two adjacent pixels in an image. The aim of correlation measures is to keep the amount of redundant information available in the encrypted image as low as possible. In general, if the correlation coefficient equals zero or is very near to zero, then the original image and its encrypted version are totally different. It can be inferred that the encrypted image has no features and is highly independent of the original image. If the correlation coefficient is equal to -1, that means the encrypted image is a negative of the original image. Correlation coefficient of the original image is usually high (close to one). Weaker the correlation coefficient of the encrypted image better the algorithm.

To examine the correlation property between two vertically adjacent pixels, two horizontally adjacent pixels, two diagonally adjacent pixels in the encrypted image, the following method is used. First, we randomly select 2000 pairs of two adjacent pixels from the image. Second, we calculate the correlation coefficient of each adjacent pair by using the following formulas,

$$\bar{A} = \frac{1}{N} \sum_{i=1}^N X_i \quad \bar{B} = \frac{1}{N} \sum_{i=1}^N Y_i \quad \dots\dots\dots[3]$$

$$r = \frac{\sum_{i=1}^N (X_i - \bar{A})(Y_i - \bar{B})}{\sqrt{\sum_{i=1}^N (X_i - \bar{A})^2 \sum_{i=1}^N (Y_i - \bar{B})^2}} \quad \dots\dots\dots[4]$$

where N is the number of adjacent pixels selected from the image to calculate the correlation in an image, X_i and Y_i are the values of adjacent pixels in the image.

Differential analysis [5] - The attacker may have a slight change (modify one pixel) of the plain image to find some meaningful relationships between the plain image and the encrypted. If one minor change in the plain image causes a significant change in the cipher image, this indicates that the encryption scheme resists differential attacks more efficiently. To test the influence of only one pixel change in the plain image over the whole encrypted image, two common measures are used: Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI). NPCR means the number of pixels change rate of encrypted image while one pixel of original image is changed. UACI measures the average intensity of the differences between the original image (plain -image) and encrypted image (ciphered image). Consider two encrypted images (cipher-images), E1 and E2, whose corresponding original images (plain-images) have only one pixel difference. The NPCR of these two images is defined as

$$NPCR = \frac{\sum_{i,j} D(i,j)}{MXN} \times 100\% \quad \dots\dots\dots[5]$$

Where

$$D(i,j) = \begin{cases} 0, & \text{if } c1(i,j) = c2(i,j) \\ 1, & \text{if } c1(i,j) \neq c2(i,j) \end{cases} \quad \dots\dots\dots[6]$$

Another measure, UACI, is defined by the following formula:

$$UACI = \frac{1}{MXN} \sum_{i,j} \left[\frac{|C1(i,j) - C2(i,j)|}{255} \right] \%100 \quad \dots\dots\dots[7]$$

Entropy Analysis - It is an important concept for analyzing an encryption scheme. Entropy gives an idea about self information. The entropy of a message *m* can be indicated as

H(*m*). If there are M symbols and p (*mi*) as the probability of occurrence of symbol *mi*, then the equation for entropy is given as:

$$H(m) = \sum_{i=0}^{M-1} p(mi) \log_2 \frac{1}{p(mi)} \quad \dots\dots\dots[8]$$

B. Evaluation of the watermarking algorithms

1) *Mean Square Error(MSE):*

It measures the average of the squares of the errors, i.e., the difference between the original values and obtained values.

$$MSE = \left[\frac{1}{MN} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} [f(x,y) - \hat{f}(x,y)]^2 \right] \quad \dots\dots\dots[9]$$

2) *Root Mean Square Error:*

It measures the square root of the MSE.

$$RMSE = \sqrt{\left[\frac{1}{MN} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} [f(x,y) - \hat{f}(x,y)]^2 \right]} \quad \dots\dots\dots[10]$$

3) *Signal to Noise Ratio (SNR):*

In order to evaluate the quality of watermarked image, the following signal-to-noise ratio (SNR) equation is used:

$$SNR = \frac{\sum_{i=0}^M \sum_{j=0}^N I^2(i,j)}{\sum_{i=0}^M \sum_{j=0}^N [I(i,j) - I_w(i,j)]^2} \quad \dots\dots\dots[11]$$

4) *Peak Signal to Noise Ratio (PSNR):*

The quality of watermarked image is measured by PSNR (Peak signal to Noise Ratio). Bigger is PSNR, better is quality of watermarked image. PSNR for image with size M x N is given by:

$$PSNR = 20 \log \left(\frac{255}{RMSE} \right) \quad \dots\dots\dots[12]$$

Where maximum pixel value of image is equal to 255 for gray scale image where pixels are represented with 8 bits.

5) *Similarity factor:*

The number of mismatched data between the embedded watermark and the extracted watermark is used to represent the similarity of watermarks. The similarity factor of extracted watermark and original watermark is computed by the following:

$$SF = \frac{\sum_{i=1}^M \sum_{j=1}^N (w(i,j)^2) * w'(i,j)}{\sqrt{\sum_{i=1}^M \sum_{j=1}^N (w(i,j)^2) * \sum_{i=1}^M \sum_{j=1}^N w}} \quad \dots\dots\dots[13]$$

Where W and W' represent the original watermark image and the extracted watermark image, respectively, M and N represent the image size. The magnitude range of SF is $[0, 1]$. If SF is near or equal to 1, the extracted watermark is more effectively extracted. In general, it is considered acceptable that SF is 0.75 or above.

V. SIMULATION RESULTS

The algorithm implementation was carried out on MATLAB/SIMULINK platform. Figure 2 shows the result of the proposed algorithm. The performance is compared with the standard AES-128 algorithm.

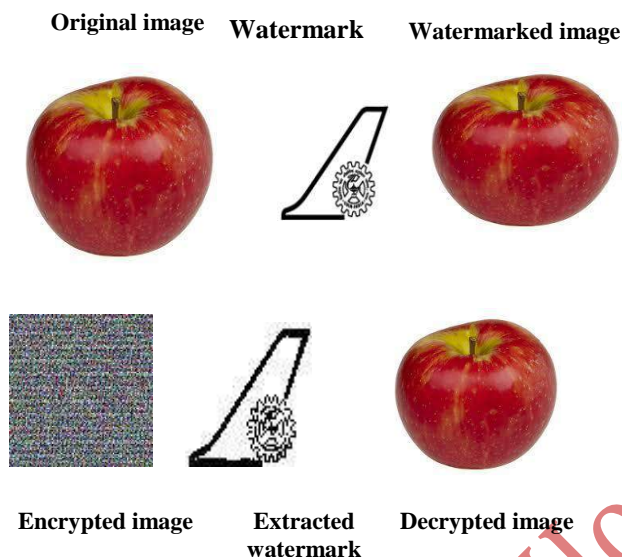


Fig. 2 Encryption and watermarking

The encryption achieved by the proposed algorithm is quantified in terms of the parameters given in the previous section and the obtained values are given below. Table I gives the correlation coefficient computed for both original and encrypted images. For these computations, 2000 adjacent pixels were selected along horizontal, vertical and diagonal directions. The results indicate that correlation in the encrypted image is very much less compared to the original image, which is very much desirable. These values are comparable to corresponding values obtained for AES encryption.

Table – I: Correlation co-efficient analysis

Image	Horizontal	Vertical	Diagonal
Original	0.992893	0.990519	0.986580
Encrypted	-0.091312	-0.304023	-0.046719

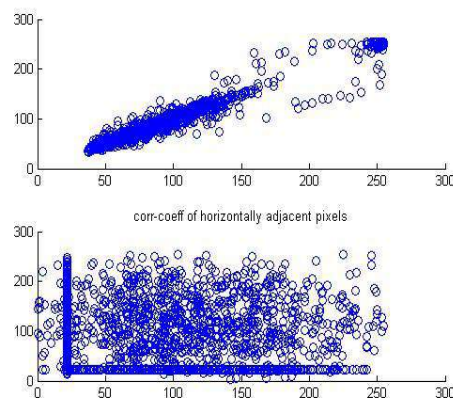


Fig. 3 Correlation plot of horizontal adjacent pixels

Figure 3 gives the correlation plot of original and encrypted images computed using horizontal adjacent pixels. This also depicts that correlation in encrypted image is less than original image. Further, the entropy analysis shows that entropy of encrypted image (6.226384) is higher than that of the original image (5.929383), as desired. The encryption quality of the proposed algorithm is 24852.53, which is better than AES(15440.16).

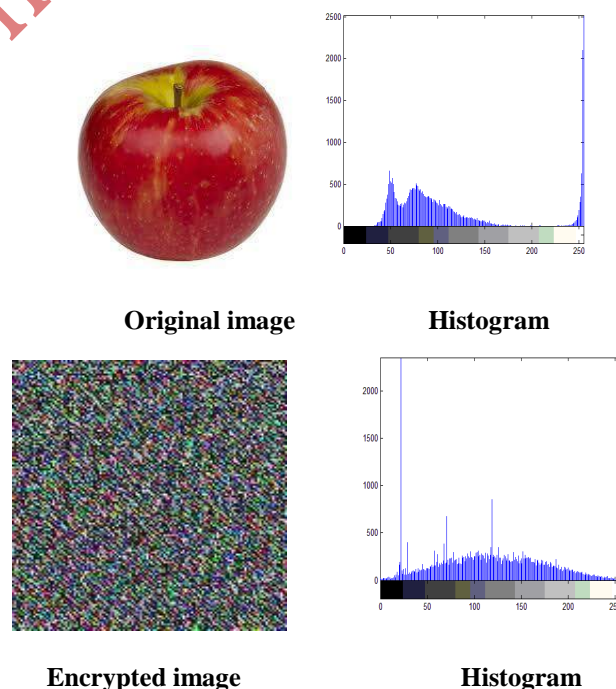


Fig. 4 Histogram analysis

Figure 4 gives the histograms of the original image and corresponding encrypted image. This depicts the histograms of both original and encrypted images are completely different. The encrypted image histogram is somewhat flat and histogram changes are less as compared to original. So that the recovery of the image from the histogram is very difficult.

The NPCR and UACI values are 0.1580% and 5.9849×10^{-4} , respectively. This shows that the algorithm is weak against differential analysis.

As far as embedding watermarking is concerned, the computed SNR, PSNR, RMSE and similarity factor are 5.35×10^4 , 9.32, $X10^4$, 0.023 and 0.999, which are satisfactory.

VII CONCLUSION

This paper proposes a joint encryption-watermarking algorithm for images. The encryption is based on Arnold transformation with S-box. This algorithm is simple and has high confidentiality. The watermark is inserted and extracted in the DCT domain. However, the proposed algorithm is vulnerable to differential attack and needs to be improved further.

References

- [1] Web link:
www.facweb.iitkgp.emet.in/~sourav/DES.pdf
- [2] Hamdan.O.Alanazi, B.B.Zaidan, A.A.Zaidan, Hamid A.Jalab, M.Shabbir and Y. Al-Nabhani, "New Comparative Study between DES, 3DES and AES within Nine Factors", Journal of computing, Volume 2, Issue 3, March 2010, ISSN 2151-9617
- [3] C. Narsimha Raju, Ganugula Umadevi, Kannan Srinathan and C. V. Jawahar, "Fast and Secure Real-Time Video Encryption", Sixth Indian IEEE Conference on Computer Vision, Graphics & Image Processing, 2008, 16-19 Dec. 2008, Bhubaneswar
- [4] M. Abomhara, Omar Zakaria, Othman O. Khalifa, "An Overview of Video Encryption Techniques", International Journal of Computer Theory and Engineering, Vol. 2, No. 1 February, 2010
- [5] Shujun Li, Xuan Zheng, Xuanqin Mou and Yuanlong Cai, "Chaotic Encryption Scheme for Real-Time Digital Video", Proc. SPIE 4666, Real-Time Imaging VI, 149 (March 4, 2002)
- [6] Saraju P. Mohanty, Elias Kougiianos, "Real-time perceptual watermarking architectures for video

broadcasting", The Journal of Systems and Software 84 (2011) 724-738

[7] Priyanka Gupta, Sonia Singh, Isha Mangal "Image Encryption Based On Arnold Cat Map and S-Box" Volume 4, Issue 8, August 2014 International Journal of Advanced Research in Computer Science and Software Engineering

[8] I. El-Fegh, D. Mustafa, Zakaria Suliman Zubi, Faraj A. El-Mouadib "Color Image Watermarking based on the DCT-Domain of Three RGB Color Channels" Proceedings of the 10th WSEAS International Conference on EVOLUTIONARY COMPUTING

[9] Saeed AL-Mansoori, and Alavi Kunhu, "Robust Watermarking Technique based on DCT to Protect the Ownership of DubaiSat- 1 Images against Attacks" IJCSNS International Journal of Computer Science and Network Security, VOL.12 No.6, June 2012

IJournals